VoteHere®

# How to Do Voting Right

Eric A. Peterson
Director of Strategic Technology
ericpe@votehere.net

## Introduction

Voting is the cornerstone in the foundation of democracy. We need our elections to be fair, accurate and private. More importantly, we need to believe that they are fair, accurate and private. There is increasing evidence that our current systems' abilities to meet those needs are built on fundamentally unsound footings, yet many still believe that the best way to ensure future election validity is to ensure that all new systems be based on those same shaky approaches.

This is most assuredly a path leading to stagnation at best, and at worst disaster.

We no longer need to, and can therefore no longer afford to rely on systems that can only imply the validity of election results from an audit of the election process, or their use of supposedly secure components and data transfers. All voting systems, old and new, must be evaluated against a fundamentally new model for establishing and proving election validity.

This paper examines some of the questions fundamental to voting, where the current models are breaking down, how a new model can address many of the problems in our current systems, and further why that new model should be a fundamental requirement for all future innovation in voting systems.

## Is 'Vote' a Verb or a Noun?

First of all, why does the answer to this question even matter? The reason is simple. If 'vote' is fundamentally an action, then the systems and processes that we use need to focus on capturing and recording the actions of all of the parties involved, preserving that record, and attempting to draw conclusions from that record. If 'vote', however, is fundamentally some 'thing' that exists independent from the actions of voting, then our systems should most correctly be focussed on capturing, preserving and tabulating those 'things'.

At first blush, many people generally conclude that 'vote' is most properly a verb. This position is understandable, given that they are generally only familiar with the process of voting. It turns out, however, that there are several reasons that this common conception is not accurate:

1. The individual's right to influence the final outcome does not derive from nor dissipate with the action of voting. If 'vote' were an action, the 'one person – one vote' principal would in all cases prohibit the individual from performing the action of voting more than once in an election. There are provisions in most voting rules that allow individuals to complete the act of voting more than once, as long as only one recording can be identified as valid. For example, a voter who can prove before the close of the election that an absentee ballot has been lost or destroyed in transit is usually given the opportunity to cast another.
2. If 'vote' were an action, the accuracy of the vote recording process (as separate from vote tabulation) could never be an issue, as by definition the recorded actions of the voter (assuming the recording itself is unaltered) would righteously and correctly be counted as their vote. Confusion over ballot layout or system mechanics could never be sited as sources

of election inaccuracy. If ‘vote’ were an action, there would be no basis for a debate over the differences between what the individual did and what the individual ‘intended’ to do. But, as was shown so publicly in Palm Beach County Florida during the 2000 presidential election, this debate does take place.

3. The actions involved in voting are necessary, but not sufficient for a valid vote to be cast and counted.
   a) In theory, performing all the acts of voting, but without the proper authorization, does not result in creating a valid vote. Of course, systems may not be able to tell the difference between those who performed the actions with authorization and those who might have been allowed to perform them without that authorization, but that in no way reduces the fact that we still view the unauthorized actions as ‘invalid votes’.
   b) In many cases, authorized and valid voters perform all of the actions, but their vote still does not end up included in the final tally. For example, military voters who “voted” and the votes were not counted because of late arrival or missing postmark, and Oregon voters who “voted” but were tricked into depositing their ballots in phony ballot boxes where they were stolen and not counted.
4. The concept of provisional voting allows all voting actions to be performed without creating a ‘real’ vote (that is, a ballot is created for an individual not yet granted the vote ‘potential’). Once the individual is vetted and granted his or her vote ‘potential’ the ballot is immediately ‘promoted’ to carry that individuals potential into the tally. Further, the ballot cast in this fashion is conceptually indistinguishable from any cast by any other individual.

Clearly, although the acts performed during the process are crucial, the key concept of a vote separate from those actions is what drives our modern view of voting.[1]

## Where Do Ballots Fit In?

For those who do initially believe that ‘vote’ is a noun, the most likely reason is that they internally equate their ballot with their vote. It is important to note, however, that this view is also flawed, and that ‘vote’ and ‘ballot’ cannot be used interchangeably.

Ballots are perhaps best described as containers for the vote. Voters ‘pour’ their vote into the ballot and the tabulation system extracts the vote from the ballot and adds it to the tally. If the voter somehow becomes aware and can prove that the container of their vote has been destroyed or lost (as can happen for example in mail-in absentee voting), most election rules recognize that the ‘vote’ itself has returned to the voter, and that individual is allowed to pour it into and cast another ballot.

Establishing this difference between votes and ballots is important. It allows us to discuss the difference between protecting the ballots and protecting the votes contained in those ballots, and to recognize the value that can be gained from systems that allow voters to check on the status of their ballot without revealing the detail of their votes.

## What is an Election System to Do?

At the highest level, election systems must do two things:

1. capture and aggregate individual votes into a tally, and
2. prove the validity of that tally.

[1] For a more thorough discussion on this topic, including a definition of what ‘vote’ as a noun really is, please refer to *The Metaphysics of Voting*, Copyright © 2001 VoteHere, Inc.

At least in public sector elections in the United State, proving the validity of the tally, and thus the election, is based primarily upon proving[2]:

1. Only valid registered voters voted.
2. All valid registered voters submitted at most one vote.
3. The tally accurately reflects all of the valid votes
4. No one can prove how any individual voted.

Conditions 1 and 2 are generally considered *fairness* provisions, condition 3 speaks to *accuracy* and condition 4 to *privacy*. Missing from this list are several buzzwords generally thought of as fundamental requirements for election systems, perhaps most notably *security*. This is not to minimize the need for system security, but simply because security is not an independent requirement. Rather, it is one derived from these fundamental four.

## What's So Hard About That?

On the surface this seems like this should be a fairly simple task. It is, however, deceptively difficult to prove fairness and accuracy while still maintaining individual privacy. It is so difficult, in fact, that none of the election systems currently in use in the United States can actually do it completely.

The fundamental problem essentially boils down to the protection of the ballot (and therefore the vote it contains) once it has been cast. At the very least, steps must be taken to ensure that a voted ballot

- cannot be read until the polls close
- cannot be changed by any single person at anytime, including vendors and election officials
- cannot be linked to the voter

Those systems that maintain ballot images generally strip all identifying voter information from the ballots very early in the process, in order to ensure the privacy requirements are met. These systems must thereafter rely on a procedural audit of all possible influences on the "anonomized" ballot. As has been shown numerous times with various forms of paper ballots, there are any number of ways that this process audit protection can break down. Ballots are unknowingly lost, maliciously modified, or even voided by the very processes and machinery of the system itself. Once separated from the voter, there is no way to verifiably establish what the ballot data "should be", and thus no way to prove that it is still valid. These systems can at best only imply that the data has remained valid and untouched throughout the election.[3]

Nor are the issues limited to paper based election systems. Typically, voted DRE ballots are also vulnerable to at least two of the risks listed above -- they can be read or changed. Electronic ballot images are typically stored on flash memory cards, where anyone who has or gains access to the system can view or change them after they have been cast. These ballots can be compromised on the DRE machine itself or on the flash memory cards that are collected from the machines for election tabulation. Anyone with access to and insider knowledge of the DRE system can accomplish this.

Finally, and perhaps most damning, due to the fundamental limitations of all procedural audit systems, there is no real way for anyone to know for sure if any of these potential problems have been encountered or not. For example, even in cases where the most conservative statistical analysis has

[2] For more precise definitions of these rules, please refer to *Establishing Election Validity*, Copyright © 2001, VoteHere, Inc.

[3] For a complete discussion of process audit and its alternative, data audit, please refer to *Establishing Election Validity*, Copyright © 2001, VoteHere, Inc.

shown the virtual certainty of ballot manipulation and fraud, the lack of absolute proof in the procedural audit trail has prevented effective prosecution or other remedies.

## In Whom Should We Trust?

The renewed attention and focus on elections has brought many new players and technologies into the arena. Companies both new and established are proposing many different solutions, with many different qualities. Where should we turn? What direction should we take? All of these questions boil down to this one: in whom should we trust?

All systems that rely on procedural audit of the election force us to trust:

1. That no external influences were able to undetectably alter the election data, and
2. That no one internally involved in the election process did anything, even inadvertently, that affected the outcome of the election.

This is true of paper election systems and most existing electronic election systems. It is equally true of many new or proposed systems, including those that run on and rely on the supposed protection of obscure data formats, private ATM networks or dedicated cable channels, but rely on procedural protection of ballots once they are delivered through the network. The key issue to recognize is that the fundamental security of the ballots really has nothing to do with ballot form or material, nor with how or even if they are transmitted over a network.

The only real way to protect the ballots and the votes they contain is to build a system that allows their validity to be proven at the end of the process, no matter who has or even just might have 'touched' them or what route they took.

So the best answer is that the system should force us to trust no one. Not no one as in nobody, but no one as in no single entity. The ideal is that our belief in the election results and the privacy of the election should not be placed in the system vendor, the system operator nor for that matter even in the election officials themselves. Not that any of these are necessarily untrustworthy, but simply that everyone with a stake in the election would be better served by being able to independently prove the validity of the results.

## Is All This Really Necessary?

There are two perspectives on answering this fundamentally subjective question. The first is rather philosophical, the second much more analytical.

Philosophically, election results in modern democracies directly or indirectly affect nearly everything. Election results determine taxes, wars, highways, houses, streets, parks, education, environment, crimes, punishments, etc. – really the entire future of society itself. Put in that context, now answer these questions:

How necessary is fairness?
How necessary is accuracy?
How necessary is privacy?

It seems very hard to argue that we should settle for 'good enough' any time a real opportunity arises to improve both the actual quality of election results and, even more importantly, the basis for our belief in those results[4].

[4] The thesis of election 'binding potential' being derived directly from belief in the validity of the election results is explored in *The Metaphysics of Voting*, Copyright © 2001, VoteHere, Inc.

Analytically, the necessities of scale, speed and convenience continue to converge to encourage or even force election systems to become automated. The most likely next innovations in election systems will take many forms, including:

- ATM like machines, standing alone or linked on private networks
- mobile devices on wireless networks
- private computers on public networks (the Internet)
- televisions on cable networks

This move to electronic data, increased centralization, and inherently opaque computing

1. indisputably magnifies the need to protect the election data and
2. simultaneously makes it impossible to perform an exhaustive process audit, as the actual processes inside the computing devices cannot be verifiably observed and recorded.

Yet, like all election systems, these new systems too must prove that the election data they transported and processed remained private and unaffected by any unauthorized influences, malicious or inadvertent, external or internal.

## Can It Be Done?

The idea of universally verifiable elections is not some abstract or unattainable ideal. The technologies developed by VoteHere are up to the challenge[5]. These systems focus attention on the *election information* itself, rather than the people, machines and mechanisms that handle it. They also distribute the authority to perform the most critical steps across any number of individuals, thus ensuring that no single party to the election process is able to independently violate the constraints and rules that govern the election.

Most importantly, they produce a complete election record – all the way from who configured and approved the ballot styles, to exactly who has voted, to the specific computation steps used to arrive at the final tally – collected and represented in such a way that not a bit of it can be altered without creating intrinsic inconsistency. With this data transcript, anyone who is interested can independently verify the validity of the election directly from the election data itself.

## Conclusion

Limitations in technology have historically forced all election systems to compromise real verifiability to protect privacy. We have lived with these compromises, perhaps in part because of the general lack of knowledge about their implications, but more certainly because we have not had a choice of anything fundamentally different or better.

The goal of elections that can be independently verified by anyone is now attainable. But to reach that goal we must first let go of the concept of auditing the election process, and turn instead to an approach that audits the election data itself. By embracing this new approach, we not only improve the accuracy, validity and belief in the way that we currently conduct elections, but we enable and benefit from new approaches to elections that would otherwise be irresponsible, certainly reckless, and perhaps even disastrous to implement any other way.

[5] Please visit http://www.votehere.net/ourtechnology.html for more complete descriptions and discussions of these technologies.